Block-groups and Hall relations*

Azza M. Gaysin[1] and Mikhail V. Volkov[2]

[1] Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovska 83, 186 00 Praha 8, Czech Republic
azza.gaysin@gmail.com
[2] Chair of Algebra and Theoretical Computer Science, Institute of Natural Sciences and Mathematics, Ural Federal University, Lenina 51, Ekaterinburg 620000, Russia
m.v.volkov@urfu.ru,
WWW home page: http://csseminar.kmath.ru/volkov/

Abstract. A binary relation on a finite set is called a Hall relation if it contains a permutation of the set. Under the usual relational product, Hall relations form a semigroup which is known to be a block-group, that is, a semigroup with at most one idempotent in each $\mathscr{R}$-class and each $\mathscr{L}$-class. Here we show that in a certain sense, the converse is true: every finite block-group divides a semigroup of Hall relations on a finite set.

Keywords: Hall relation, reflexive relation, $\mathscr{J}$-trivial semigroup, block-group, power semigroup, semidirect product, semigroup division

1 Background and Motivation: Straubing's Theorem

The result that we are going to present is inspired by Straubing's representation theorem for $\mathscr{J}$-trivial monoids [19]. Straubing's theorem involves three notions: $\mathscr{J}$-trivial semigroups, monoids of reflexive relations, and semigroup division. For the reader's convenience, we recall their definitions.

Given a semigroup S, we denote by S^1 the least monoid containing S, that is, $S^1 := S$ if S has an identity element and $S^1 := S \cup \{1\}$ if S has no identity element; in the latter case the multiplication in S is extended to S^1 in a unique way such that the fresh symbol 1 becomes the identity element in S^1. Green [6] defined five important equivalencies on every semigroup S, collectively referred to as *Green's relations*, of which we meet the following three in this note:

$x \mathscr{R} y \Leftrightarrow xS^1 = yS^1$, i.e., x and y generate the same right ideal;
$x \mathscr{L} y \Leftrightarrow S^1x = S^1y$, i.e., x and y generate the same left ideal;
$x \mathscr{J} y \Leftrightarrow S^1xS^1 = S^1yS^1$, i.e., x and y generate the same ideal.

Basic information about $\mathscr{R}$, $\mathscr{L}$, and $\mathscr{J}$ can be found in the early chapters of any general semigroup theory text such as, e.g., [5,10], but actually this note uses only the above definitions of these three relations.

* Supported by the Ministry of Science and Higher Education of the Russian Federation (Ural Mathematical Center project No. 075-02-2020-1537/1)

A semigroup S is said to be *$\mathscr{J}$-trivial* if the relation $\mathscr{J}$ on S coincides with the equality relation Δ_S on S. In other words, this means that the following implication holds for all $x, y \in S$:

$$S^1xS^1 = S^1yS^1 \to x = y.$$

Let X be a set. Recall that binary relations on X are multiplied as follows: for $\rho, \sigma \subseteq X \times X$, their product is set to be the relation

$$\rho\sigma := \{(x, y) \in X \times X \mid \exists z \in X\ (x, z) \in \rho\ \&\ (z, y) \in \sigma\}.$$

This multiplication is associative and Δ_X, the equality relation on X, serves as the identity element for it. Thus, the binary relations on X constitute a monoid. Also, it is easy to check that the multiplication is compatible with inclusions between relations: if $\rho \subseteq \rho'$ and $\sigma \subseteq \sigma'$, then $\rho\sigma \subseteq \rho'\sigma'$.

A binary relation ρ on X is *reflexive* if ρ contains Δ_X. The above observations immediately imply that the reflexive relations on X form a submonoid in the monoid of all binary relations on X. Let $\mathcal{R}_n$ denote the monoid of all reflexive binary relations on a set with n elements. This monoid can be conveniently thought of as a submonoid of the monoid of all $n \times n$ matrices (with the usual matrix multiplication) over the Boolean semiring $\{0, 1\}$, with the operations $+$ and $\cdot$ on $\{0, 1\}$ being defined by the rules:

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0 + 0 = 0, \qquad 1 \cdot 1 = 1 + 0 = 0 + 1 = 1 + 1 = 1.$$

Namely, $\mathcal{R}_n$ can be identified with the submonoid consisting of matrices in which all diagonal entries are 1.

Finally, a semigroup S is said to *divide* another semigroup T if S is a homomorphic image of a subsemigroup in T. Now we are in a position to formulate Straubing's theorem.

Theorem 1 (Straubing [19]). *A finite semigroup S is $\mathscr{J}$-trivial if and only if S divides the monoid $\mathcal{R}_n$ for some n.*

Remark 1. In [19], the above result is stated for S being a monoid; this makes no essential difference since S is $\mathscr{J}$-trivial if and only if so is S^1.

Theorem 1 looks quite innocent as it is stated in purely semigroup-theoretic terms and very much resembles textbook representation results such as the Cayley-type representation of arbitrary semigroups by transformations or binary relations. However, no direct semigroup-theoretic proof of Theorem 1 is known. The proof in [19] crucially depends on Simon's theorem [15,16], a deep combinatorial result in the theory of recognizable languages. Moreover, it can be shown relatively easily that Theorem 1 and Simon's theorem are equivalent, and therefore, a direct proof of the former would provide a new algebraic proof of the latter. In the literature, there are many proofs of Simon's theorem, based of different techniques, but none of the proofs are purely algebraic.

In the present note, we provide a representation by binary relations for another, larger class of finite semigroups, namely, the class of all finite block-groups. We introduce and briefly discuss this class in Section 2, while in Section 3 we present a family $\{\mathcal{H}_n\}$ of monoids of binary relations consisting of so-called Hall relations. Our main result, which is stated and proved in Section 4, shows that the family $\{\mathcal{H}_n\}$ plays for block-groups precisely the same role as the family $\{\mathcal{R}_n\}$ plays for $\mathscr{J}$-trivial semigroups.

2 Block-Groups and Power Semigroups of Groups

Recall that an element e of a semigroup S is said to be an *idempotent* if $e^2 = e$. A *block-group* is a finite semigroup with at most one idempotent in each $\mathscr{R}$-class and each $\mathscr{L}$-class. This definition can be expressed by the following implications:

$$ef = e^2 = e \;\&\; fe = f^2 = f \to e = f, \tag{1}$$

$$ef = f^2 = f \;\&\; fe = e^2 = e \to e = f. \tag{2}$$

Indeed, (1) and respectively (2) express the facts that any $\mathscr{R}$-related (respectively, $\mathscr{L}$-related) idempotents coincide.

We refer the reader to Pin's enthusiastic survey [14] for an explanation of the name "block-group". The survey presents also remarkable and profound connections between block-groups and the theory of recognizable languages, especially its topological aspects. An unexpected connection of block-groups to computational complexity theory has been established in [3].

While the "external" connections just mentioned are of definite importance and interest, the present note is entirely "internal" with respect to the algebraic theory of block-groups. We need two results of this theory. The first one, due to Margolis and Pin [12], relates block-groups to $\mathscr{J}$-trivial semigroups.

Proposition 1 ([12], Proposition 2.3). *A finite semigroup S is a block-group if and only if the idempotents of S generate a $\mathscr{J}$-trivial subsemigroup in S.*

Remark 2. In [12], the above result is stated for S being a monoid; this makes no essential difference since S is a block-group if and only if so is S^1. The same remark applies also to Theorem 2 below, which also was originally stated for the case of monoids.

Given a semigroup S, we denote by $\mathcal{P}(S)$ the set of all its non-empty subsets. One introduces an associative multiplication on $\mathcal{P}(S)$ as follows: the product of subsets $A, B \in \mathcal{P}(S)$ is the subset

$$AB := \{ab \mid a \in A,\ b \in B\}.$$

Then $\mathcal{P}(S)$ becomes a semigroup which is called the *power semigroup of S*.

A jewel of the theory of block-groups is their characterization in terms of power semigroups of groups. This deep and difficult result is due to Henckell and Rhodes [9], see also [8] for a detailed explanation and [20,1] for modern and shorter (but still complicated) proofs.

Theorem 2. *A finite semigroup S is a block-group if and only if S divides the power semigroup of some finite group.*

Here we make a comment similar to that made after Theorem 1: even though the formulation of Theorem 2 is purely semigroup-theoretic, all its proofs in the literature employ tools from outside algebra.

3 Hall relations

A binary relation $\rho \subseteq X \times X$ on a finite set X is called a *Hall relation* if ρ contains a permutation of X. Here we treat permutations as binary relations, that is, given a permutation $\pi\colon X \to X$, we identify it with the relation $\{(x, x\pi) \mid x \in X\}$.

The name "Hall relation" was coined by Schwarz [17,18] with the reference to the classic marriage theorem by Hall [7]. Indeed, Hall's theorem deals with perfect matchings in bipartite graphs, and if one represents binary relations on a finite set as bipartite graphs, Hall relations are precisely those whose graphs admit a perfect matching. In the representation of binary relations as matrices over the Boolean semiring, Hall relations correspond to matrices with permanent 1.

The product of two permutations considered as relations on X coincides with their usual product in the group of all permutations on X. If ρ, ρ' are Hall relations and π, π' are permutations such that $\pi \subseteq \rho$ and $\pi' \subseteq \rho'$, the product $\rho\rho'$ contains the permutation $\pi\pi'$ whence $\rho\rho'$ is a Hall relation again. Since Δ_X, the equality relation on X, is a Hall relation, the Hall relations on X form a submonoid in the monoid of all binary relations on X. Let $\mathcal{H}_n$ denote the monoid of all Hall relations on the set $X_n := \{1, 2, \ldots, n\}$. Clearly, $\mathcal{H}_n$ contains both the monoid $\mathcal{R}_n$ of all reflexive relations on X_n and the group $\mathbb{S}_n$ of all permutations on X_n.

The monoid $\mathcal{H}_n$ turns out to be a block-group. This property of $\mathcal{H}_n$ can be extracted from results announced by Ki Hang Kim [4][1]. The argument outlined in [4] is of counting nature: the author exhibits a recursive formula for the number of idempotents in $\mathcal{H}_n$ [4, Theorem 15], and then he claims that the number coincides with both the number of $\mathscr{L}$-classes that contain idempotents and the number of $\mathscr{R}$-classes that contain idempotents [4, Corollary 17]. The research announcement [4] contained no proofs, nor we found any proofs of claims made therein in later publications that dealt with monoids of Hall relations. Therefore, we include here a short counting-free argument.

Proposition 2. *The monoid $\mathcal{H}_n$ is a block-group.*

Proof. Let ρ be an idempotent from $\mathcal{H}_n$ and π a permutation contained in ρ. There exists a positive integer k such that $\pi^k = \Delta_{X_n}$. Since $\rho^2 = \rho$, we have $\rho = \rho^k \supseteq \pi^k$, whence $\rho \supseteq \Delta_{X_n}$. Thus, ρ is reflexive, and we have shown that every idempotent of $\mathcal{H}_n$ lies in $\mathcal{R}_n$. The latter monoid is $\mathscr{J}$-trivial, and hence, $\mathcal{H}_n$ is a block-group by Proposition 1. □

[1] This paper was published under the name Kim Ki-hang Butler; see the biography of Ki Hang Kim [2] for an explanation.

4 Representation Theorem

Theorem 3. *A finite semigroup S is a block-group if and only if S divides the monoid $\mathcal{H}_n$ for some n.*

Proof. The class of all block-groups is known to be closed under division (see, e.g., [12]). Therefore the "if" part immediately follows from Proposition 2.

For the "only if" part, we employ Theorem 2. Choose a finite group G such that S divides $\mathcal{P}(G)$ and let $n := |G|$. It is sufficient to show that the semigroup $\mathcal{P}(G)$ embeds into the monoid $\mathcal{H}_n$. In order to simplify notation, we identify G and X_n as sets. Now, for each non-empty subset $A \in \mathcal{P}(G)$, define a binary relation ρ_A as follows:

$$\rho_A := \{(g, h) \in G \times G \mid g^{-1}h \in A\}.$$

Fix an element $a \in A$. By the definition, ρ_A contains all pairs (g, ga), where g runs over G. As the relation $\{(g, ga) \mid g \in G\}$ is a permutation of G, we see that ρ_A is a Hall relation. Thus, the map $f\colon A \mapsto \rho_A$ sends $\mathcal{P}(G)$ into $\mathcal{H}_n$.

We aim to show that $f\colon \mathcal{P}(G) \to \mathcal{H}_n$ is an embedding of semigroups. To see that f is one-to-one, take any two different subsets $A, B \in \mathcal{P}(G)$. Without any loss, we may assume that $A \not\subseteq B$. If $a \in A \setminus B$, the pair (e, a), where e is the identity element of the group G, belongs to ρ_A but not to ρ_B. Thus, $\rho_A \neq \rho_B$.

It remains to verify that f is a homomorphism, that is, $\rho_A\rho_B = \rho_{AB}$ for arbitrary subsets $A, B \in \mathcal{P}(G)$. If $(x, y) \in \rho_A\rho_B$, there must exist an element z such that $(x, z) \in \rho_A$ and $(z, y) \in \rho_B$. By the definition, we have $x^{-1}z \in A$ and $z^{-1}y \in B$, whence $x^{-1}y = x^{-1}z \cdot z^{-1}y \in AB$. We see that $(x, y) \in \rho_{AB}$. Thus, $\rho_A\rho_B \subseteq \rho_{AB}$.

To prove the opposite inclusion, take $(g, h) \in \rho_{AB}$. Then $g^{-1}h \in AB$, that is, $g^{-1}h = ab$ for some $a \in A$ and $b \in B$. We see that $g^{-1}hb^{-1} = a$, whence $(g, hb^{-1}) \in \rho_A$, while $(hb^{-1})^{-1}h = b$, whence $(hb^{-1}, h) \in \rho_B$. Therefore, we get $(g, h) \in \rho_A\rho_B$, as required. □

As the above proof shows, Theorem 3 is rather a straightforward consequence of Henckell and Rhodes's theorem (Theorem 2). After the formulation of Straubing's theorem (Theorem 1) in Section 1, we said that it is more than a consequence of Simon's theorem: Theorem 1 is in fact equivalent to Simon's theorem whence a direct algebraic proof of the former would provide a new algebraic proof of the latter. Could the same be said about the relationship between Theorem 3 and Henckell and Rhodes's theorem?

To address this question, we need the concept of the semidirect product of a monoid with a group. Let M be a monoid, G a group, $\operatorname{Aut} M$ the automorphism group of M, and $\alpha\colon G \to \operatorname{Aut} M$ a group homomorphism. For $m \in M$ and $g \in G$ we write gm for the image of m under the automorphism $g\alpha$ (so that we assume that automorphisms act on the left). The *semidirect product* $M \rtimes G$ with respect to α is the set $M \times G$ equipped with the following multiplication: for all $m, m' \in M$, $g, g' \in G$,

$$(m, g)(m', g') := (m(gm'), gg')\,.$$

The multiplication is easily seen to be associative so that $M \rtimes G$ is a semigroup.

The following result was first proved by Margolis and Pin [12, Propositions 3.6 and 3.7] by language-theoretical tools. Pin [14] asked for its purely semigroup-theoretic proof. Such a proof was then published by Auinger and Steinberg [1].

Proposition 3. *Every semidirect product of a finite $\mathscr{J}$-trivial monoid with a finite group divides the power semigroup of some finite group.*

Now we register a further property of monoids of Hall relations. As mentioned, the monoid $\mathcal{H}_n$ contains both the monoid $\mathcal{R}_n$ and the group $\mathbb{S}_n$. Observe that $\mathbb{S}_n$ acts on $\mathcal{R}_n$ by conjugation since the relation $\pi\rho\pi^{-1}$ is reflexive for every $\rho \in \mathcal{R}_n$ and every $\pi \in \mathbb{S}_n$. This defines a group homomorphism $\mathbb{S}_n \to \operatorname{Aut} \mathcal{R}_n$ that gives rise to the semidirect product $\mathcal{R}_n \rtimes \mathbb{S}_n$.

Proposition 4. *The monoid $\mathcal{H}_n$ is a homomorphic image of the semidirect product $\mathcal{R}_n \rtimes \mathbb{S}_n$.*

Proof. Define a map f on $\mathcal{R}_n \rtimes \mathbb{S}_n$ by $(\rho, \pi)f := \rho\pi$ for every pair $(\rho, \pi) \in \mathcal{R}_n \times \mathbb{S}_n$. Since ρ contains the equality relation, the product $\rho\pi$ contains the permutation π whence $\rho\pi$ is a Hall relation. Thus, the map f sends $\mathcal{R}_n \rtimes \mathbb{S}_n$ into $\mathcal{H}_n$.

We aim to show that $f\colon \mathcal{R}_n \rtimes \mathbb{S}_n \to \mathcal{H}_n$ is an onto homomorphism. If $\sigma \in \mathcal{H}_n$ is an arbitrary Hall relation, take a permutation τ such that $\tau \subseteq \sigma$ and consider the relation $\sigma\tau^{-1}$. Clearly, $\sigma\tau^{-1}$ is reflexive and $\left(\sigma\tau^{-1}, \tau\right) f = \sigma\tau^{-1}\tau = \sigma$. Thus, the map f is surjective.

It remains to verify that f is a homomorphism. Taking any $\rho, \rho' \in \mathcal{R}_n$ and any $\pi, \pi' \in \mathbb{S}_n$, we see that

$$\begin{aligned}
((\rho, \pi)(\rho', \pi'))\, f &= \left((\rho(\pi\rho'\pi^{-1}), \pi\pi')\right) f && \text{by definition of semidirect product} \\
&= \rho(\pi\rho'\pi^{-1})\pi\pi' && \text{by definition of the map } f \\
&= \rho\pi\rho'\pi' \\
&= ((\rho, \pi))\, f \cdot (\rho', \pi'))\, f && \text{by definition of the map } f.
\end{aligned}$$

□

Now we can easily deduce the "only if" of Theorem 2 from Theorem 3. (The "if" part of Theorem 2 is immediately ensured by the fact that power semigroups of finite groups are block-groups—see, e.g., [13, Proposition 2.4] for this fact.) Let S be a block-group. Combining Theorem 3 and Proposition 4, we see that S divides a semidirect product of a finite $\mathscr{J}$-trivial monoid with a finite group, while Proposition 3 tells us that any such product divides the power semigroup of another finite group. The division relation is transitive, whence S divides the power semigroup of the latter group.

As mentioned, there exists a purely semigroup-theoretic proof of Proposition 3. Therefore, a direct algebraic proof of Theorem 3 would provide a new algebraic proof of Henckell and Rhodes's theorem. Thus, the relationship between our main result and Henckell and Rhodes's theorem is to a large extent parallel to that between Straubing's and Simon's theorems.

We conclude with reminding a longstanding open question concerning Hall relations [11, Problem 13]: what is the cardinality of the monoid $\mathcal{H}_n$?

References

1. Auinger, K., Steinberg, B.: Constructing divisions into power groups. Theor. Comput. Sci. **341**(1-3), 1–21 (2005). doi:10.1016/j.tcs.2004.12.027
2. Boyle, M.: Remembering Ki Hang Kim. Acta Appl. Math. **126**, 3–5 (2013). doi:10.1007/s10440-013-9802-y
3. Bulatov, A., Jeavons, P., Volkov, M.: Finite semigroups imposing tractable constraints. In: Gomes, G.M.S., Pin, J.-É., Silva, P.V. (eds.) Semigroups, Algorithms, Automata and Languages. Papers from the Thematic Term held in Coimbra, May–July 2001, pp. 313–329. World Scientific, River Edge (2002). doi:10.1142/9789812776884_0011
4. Butler, K.K.H.: The semigroup of Hall relations. Semigroup Forum **9**(3), 253–260 (1974). doi:10.1007/BF02194854
5. Clifford A.H., Preston G.B.: The Algebraic Theory of Semigroups, Vol. I. (Mathematical Survey No 7(I)) American Mathematical Society, Providence (1961)
6. Green, J.A.: On the structure of semigroups. Ann. Math. (2) **54**(1), 163–172 (1951). doi:10.2307/1969317
7. Hall, Ph.: On representatives of subsets, J. London Math. Soc. **10**(1): 26–30 (1935). doi:10.1112/jlms/s1-10.37.26
8. Henckell, K., Margolis, S.W., Pin, J.-É., Rhodes, J.: Ash's Type II Theorem, profinite topologies and Malcev products. Int. J. Algebra and Computation **1**(4), 411–436 (1991). doi:10.1142/S0218196791000298
9. Henckell, K., Rhodes, J.: The theorem of Knast, the PG = BG and Type II Conjectures. In: Rhodes, J. (ed.) Monoids and Semigroups with Applications, pp. 453–463. World Scientific, Singapore (1991)
10. Howie J.M.: Fundamentals of Semigroup Theory. Clarendon Press, Oxford (1995)
11. Kim, K. H.: Boolean Matrix Theory and Applications. (Monographs and Textbooks in Pure and Applied Mathematics, 70) Marcel Dekker, New York (1982)
12. Margolis, S.W., Pin, J.-É.: Varieties of finite monoids and topology for the free monoid. In: Byleen, K., Jones, P., Pastijn, F. (eds.) Proceedings of the 1984 Marquette Conference on Semigroups, pp. 113–129, Marquette Univ., Milwaukee (1985)
13. Pin, J.-É.: Variétés de langages et monoïde des parties. Semigroup Forum **20**, 11–47 (1980). doi:10.1007/BF02572667
14. Pin, J.-É.: $BG = PG$, a success story. In: Fountain, J. (ed.) Semigroups, Formal Languages and Groups. NATO ASI Ser., Ser. C: Math. Phys. Sci., vol. 466, pp. 33–47. Kluwer Academic Publishers, Dordrecht–Boston–London (1995)
15. Simon, I.: Hierarchies of Events of Dot-Depth One, Ph. D. Thesis, University of Waterloo (1972)
16. Simon, I.: Piecewise testable events. In: Barkhage, H. (ed.) Automata Theory and Formal Languages, 2nd GI Conference, Kaiserslautern, May 20–23, 1975. LNCS, vol. 33, pp. 214–222. Springer, Heidelberg (1975). doi:10.1007/3-540-07407-4_23
17. Schwarz, Š.: On some semigroups in combinatorics. In Mini-Conference on Semigroup Theory. Held in Szeged, August 29–September 1, 1972, pp. 24–31. József Attila Univ., Szeged (1972)
18. Schwarz, Š.: The semigroup of fully indecomposable relations and Hall relations. Czechoslovak Math. J. **23**(1), 151–163 (1973)
19. Straubing, H.: On finite $\mathscr{J}$-trivial monoids. Semigroup Forum 19(1), 107–110 (1980). doi:10.1007/BF02572507

20. Steinberg, B.: PG=BG: redux. In: Smith, P., Giraldes, E., Martins, P. (eds.) Semigroups. Proceedings of the International Conference, Braga, Portugal, 18–23 June 1999, pp. 181–190. World Scientific, River Edge (2000). doi:10.1142/9789812792310_0015